By Musgrave et al:

(1) "each of the end terminals transmitting a transaction request message containing biometrics data of a user and a user identifier of said user to a communications network". However, the Examiner states that this feature is disclosed by Glass et al. alleging that Glass et al. teaches the biometric data is transferred from one computer over an unsecured network to another computer for identification or verification of a user, citing col. 3, lines 45-50. Applicants respectfully traverse this assertion.

As indicated by the Examiner's comments, or lack thereof, the Examiner has not provided disclosure in Glass et al. as to where a user identifier is included in a transaction request message. Glass et al. is related to secure transmission of biometric data over a network (see Abstract). In particular, preventing a photo of a user from being tampered with or substituted during transmission (see col. 2, lines 27-35). Glass et al. transmits a photo image as well as a code related to the image (see col. 5, lines 46-66). The photo image or associated code are not user identifiers as claimed.

(2) "and transmitting an authentication request message containing said biometrics data and said user identifier to said network". The Examiner states that this feature is shown by Glass et al. where "the file with code is output to a network for transfer to an authentication server system", citing col. 3, lines 51-59. Applicants respectfully traverse this assertion.

Claim 1 recites that this feature is performed by the electronic commerce service provider (ECSP). In the Examiner's scenario, in Glass et al., the camera image sent to the network would

be from an "end terminal" rather than form an ECSP. Further, again, as discussed above, there is no disclosure of the user identifier in Glass et al.

(3) "and an authentication server having a database for mapping a plurality of registered biometrics data to a plurality of corresponding registered user identifiers, the authentication server receiving the authentication request message via said network comparing the received biometrics data to one of the registered biometrics data which is mapped in said database to the user identifier contained in said authentication request message". The Examiner states that this feature is shown in Glass et al. where the camera certification authority may be a single data base residing within the authentication server or it may reside in a separate computer, citing col. 4, lines 14-17. Applicants respectfully traverse this assertion.

Specifically, the camera certification authority cited in this section of Glass et al. relates to authenticating that the photo image has not been tampered with, and not for comparing biometrics data as recited in claim 1.

Accordingly, for these several reasons, claim 1 is allowable, as well as independent claims 11, 20, and 22 which also includes similar features. The remaining claims are allowable at least based on their respective dependence on the independent claims.

Claim 3 recites a feature where the ECSP includes a conversion table for mapping user identifiers. The Examiner now states that this feature is disclosed by Glass et al. at col. 4, lines 14-17 where the camera certification authority may be a single database residing within the authentification server or it may reside in a separate computer. Applicants respectfully traverse this rejection. As noted above, the camera certification authority of Glass et al. verifies that the

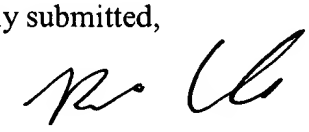
image has not been tampered with and is not used for comparing biometric data. Further, the secret key used by the camera certification authority would not correspond to a user identity as claimed.

Claim 4 recites a feature "wherein each of said end terminals is configured to cipher the biometrics data with a secret key generated by a variable secret key generator which generates secret keys which vary with time, the generated secret key being agreed-upon with said authentication server". The Examiner states that this feature is taught in Glass et al., col. 3, lines 60-67, by the token generator. Applicants respectfully traverse this rejection. As noted, the claim states that the generated secret key being agreed-upon with said authentication server. In Glass et al, however, the authentification server consults the camera certification authority each time a new image is received so that it has knowledge of the secret key corresponding to the sending camera (col. 3, lines 60-67). This consultation with the camera certification authority suggests quite the opposite than that claimed. That is, Glass et al. teaches that the authentication server as cited by the Examiner is in a passive role with regards to the secret key. This feature is also recited in claim 12.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



Ronald Kimble
Registration No. 44,186

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: July 21, 2005